Docket No. YOR919990137US1
YOR.080

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Andrea CALIFANO, et al.

Serial No.: 09/457,732	Group Art Unit: 2131
Filed: December 10, 1999	Examiner: La Forgia, Christian A.

For: SEMIOTIC SYSTEM AND METHOD WITH PRIVACY PROTECTION

Honorable Commissioner of Patents
Alexandria, VA 22313-1450

CORRECTED APPELLANTS' BRIEF ON APPEAL

Sir:

A Response to Non-Compliant Appeal Brief is submitted herewith, in which Appellants note that the Notification of Non-Compliant Appeal Brief has been rendered moot, and should be withdrawn. Notwithstanding the above, Appellants submit the Corrected Appellants' Brief on Appeal to ensure compliance with the Notification of Non-Compliant Appeal Brief.

Appellants respectfully appeal the final rejection of Claims 1 and 5-36 in the Office Action dated March 7, 2006. A Notice of Appeal was timely filed on July 7, 2006.

I. REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, assignee of 100% interest of the above-referenced patent application.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, Appellants' legal representative or Assignee which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1 and 5-36 are all the claims presently pending in the application, and are set forth fully in the attached Appendix. Claims 1, 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 are independent claims. Claims 6-8, 10-14, 16, 18, 20-23, 25, 26, 28, 30, 32, 34, and 36 are dependent claims.

Claims 2-4 stand canceled.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility.

Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza (U.S. Patent No. 6,446,210) in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

Appellants respectfully appeal the rejection of Claims 1, 14-16, 31, and 32 under 35 U.S.C. § 101, and the rejection of Claims 1 and 5-36 under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon, which are the sole issues in this Appeal.

IV. STATUS OF AMENDMENTS

An Request for Reconsideration under 37 C.F.R. § 1.116 was filed on May 8, 2006. No claims were amended.

An Advisory Action mailed June 8, 2006, stated both that the Request for Reconsideration under 37 C.F.R. § 1.116 would not be entered (see Advisory Action at paragraph 7), and also stated that the Request for Reconsideration under 37 C.F.R. § 1.116 had been considered (see Advisory Action at paragraph 11), but held Claims 1 and 5-36 unpatentable.

A Petition for a New Office Action, which properly responded to each of Appellants' traversal positions and answered the substance of those arguments, was filed on May 8, 2006. A Decision on Petition for Supervisory Review under 37 C.F.R. § 1.181 was mailed on June 22, 2006, which dismissed the Petition and noted that the differences of opinion were appealable, rather than petitionable.

A Notice of Appeal was filed timely on July 7, 2006, together with a petition for one-month extension of time.

Therefore, the claims are pending as set forth in the Appendix, as of the Request for Reconsideration under 37 C.F.R. § 1.111 filed on December 16, 2005.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

With reference to Figures 1-8, the unique and unobvious aspects of the present invention provide a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in independent Claim 1) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a function h (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), and obtaining a sample of P' such that a comparison can be made (e.g., see specification at page 13, lines 18-20; see also Figure 2, reference numeral 201), at least one of obtaining and computing h(P') (e.g., see specification at page 13, lines 20-21; see also Figure 2, reference numeral 202), and to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of the data set P (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), wherein the semiotic data includes biometric data (e.g., see Figure 1, 101; Figure 2, 201), wherein the function h includes a secure hash function (e.g., see specification at page 13, lines 3-6), wherein the data set P is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), wherein each reading gives a number Pi (e.g. see specification at page 16, lines 8-11), wherein i is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein P0 is for an initial reading (e.g. see specification at page 16, lines 8-9), and a secret version of the initial reading is stored after further processing thereof (e.g. see specification at page 16, lines 8-11), wherein reading P0 is different from Pi for i > 0 (e.g. see specification at page 16, line 12), and the secret version of P0 is different from the secret version of Pi (e.g. see specification at page 16, lines 13-14), such that no identification is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17). The method defined by claim 1, further includes extracting sub-collections Sj from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14), comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections Sj with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection Sj matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4), each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12), wherein for a plurality of users of the same biometric information, the biometric information is encrypted differently for each user (e.g. see specification at page 12, lines 18-20), and wherein at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in independent Claim 5) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a function h (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), the method further includes selecting a private key/public key (K, k) once for all cases (e.g., see specification at page 14, lines 6-7, and one of destroying the private key K and sending the private key K to a trusted party (e.g., see specification at page 14, 7-9), and choosing the function h as the public encryption function corresponding to k (e.g., see specification at page 14, lines 9-11).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 6) the data set P cannot be extracted from h(P), except by the trusted party (e.g., see specification at page 13, lines 13-14; page 14, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 7), the method further includes, to determine whether some P' is a predetermined subject, comparing the h(P') to available h(P)s (e.g., see specification at page 14, lines 13-15), and determining whether there is a match (e.g., see specification at page 14, line 15).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 8) the trusted party includes a panel of members (e.g., see specification at page 14, lines 16-20), and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret (e.g., see specification at page 14, lines 16-20).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 9) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a function h (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), wherein the data set P is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), wherein each reading gives a number Pi (e.g. see specification at page 16, lines 8-11), wherein i is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein P0 is for an initial reading (e.g. see specification at page 16, lines 12-14), and a secret version of the initial reading is stored after further processing thereof (e.g. see specification at page 16, lines 8-11), wherein reading P0 is different from Pi for i > 0 (e.g. see specification at page 16, line 12), and the secret version of P0 is different from the secret version of Pi (e.g. see specification at page

16, lines 13-14), such that no identification is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 10), the method further includes extracting sub-collections Sj from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 11), the method further includes comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections Sj with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection Sj matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 12), the method further includes, each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 13), for a plurality of users of the same biometric information, the biometric information is encrypted differently for each user (e.g. see specification at page 12, lines 18-20).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 14), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 15), is directed to a method of processing biometric data (e.g., see Figures 1-4), which includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting, with one of a secure hash function and an identity function, each the at least one data set acquired (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each of the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether the data set P' substantially matches, but does not exactly match, the at least one encrypted data set stored in the database (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 16), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 17), is directed to a method of extracting components of biometric data which are stable under measurement errors, which includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 18), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 19), is directed to a method of extracting components of biometric data which are stable under measurement errors, includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections Sj from the collection of data in the data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 20), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 21), the method further includes comparing encrypted versions of the sub-collections Sj with those data stored in the database (e.g. see specification at page 17, lines 2-6; Figure 3, 302), wherein if one or more of the sub-collection Sj matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 22), a data set P is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), such that each reading gives a number Pi (e.g., see specification at page 16, lines 4-8), wherein i is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein P0 is for an initial reading (e.g. see specification at page 16, lines 8-9), and a secret version of the initial reading is stored after further processing thereof (e.g.

see specification at page 16, lines 8-11), wherein reading P0 is different from Pi for i > 0 (e.g. see specification at page 16, line 12), and the secret version of P0 is different from the secret version of Pi (e.g. see specification at page 16, lines 13-14), such that no identification is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 23), the method further includes each time a data set is read Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 24), is directed to a system for processing semiotic data, which includes means for receiving semiotic data including a data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, Figure 3, reference numeral 301, Figure 7, reference numeral 718), means for selecting a function h, and for each the data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102; Figure 7, 711), means for destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral

103; Figure 7, 711), means for storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104; Figure 7, 718), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is close to a predetermined subject, means for comparing h(P') to available h(P)s to determine whether data set P' is close to some P (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15; see Figure 7, 711).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 25), the semiotic data includes biometric data (e.g., see Figure 1, 101; Figure 2, 201).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 26), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 27), is directed to a system for verifying biometric data without storing unencrypted biometric data, includes means for acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, Figure 3, reference numeral 301; Figure 7, 718), means for encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102; Figure 7, 711), means for destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103; Figure 7, 711), means for storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104; Figure 7, 718), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and means for comparing an encrypted data set of a data set P' to the at least one encrypted data set of data set P to determine whether there is a match and to determine whether the data set P' is a predetermined subject (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15; See Figure 7, 711).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 28), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 29), is directed to a system (e.g., see Figure 7) for extracting components of biometric data which are stable under measurement errors, includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections Sj from the collection of data in the data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 30), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 31) is directed to a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented processing biometric data, in which the method includes receiving biometric data including a data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a secure hash function h, and for each data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether data set P' is close to some data set P.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 32), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 33), is directed to a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented verifying of biometric data without storing unencrypted biometric data, the method includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is close to a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set to determine whether data set P' is close to some data set P.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 34), at least one of the data set P and P' includes a personal data set.

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 35) is directed to a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented extracting components of biometric data which are stable under measurement errors, the method includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections Sj from the collection of data in the data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 36), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for review by the Board of Patent Appeals and Interferences are whether Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101, and Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon.

VII. ARGUMENT

A. THE EXAMINER'S POSITION

In the Advisory Action mailed June 8, 2006, the Examiner stated both that the Request for Reconsideration under 37 C.F.R. § 1.116 would not be entered (see Advisory Action at paragraph 7), and also stated that the Request for Reconsideration under 37 C.F.R. § 1.116 had been considered (see Advisory Action at paragraph 11), but held Claims 1 and 5-36 unpatentable for the reasons previously identified in the final Office Action (see Advisory Action at Continuation of 11).

The Examiner maintained that Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101, and that Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon.

B. APPELLANTS' POSITION

For at least the foregoing reasons, Appellants respectfully disagree with the Examiner's positions, and therefore, Appellants traverse each of the Examiner's rejections.

1. OFFICE ACTION DOES NOT RESPOND TO, OR ANSWER THE SUBSTANCE OF, APPELLANTS' TRAVERSAL POSITIONS

It is noted that the Examiner's Response to Arguments in the March 7, 2006 Office Action was identical to the previous Response to Arguments in the September 16, 2005 Office Action, except for stating that:

> *The Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands.*

(see Office Action mailed March 7, 2005, at page 2, paragraph 5).

However, the Examiner did not state *why* or *how* the evidence presented by Applicants, or for that matter, the specifically identified disclosures in the present application which clearly contradict the Examiner's interpretation of the invention, and which clearly rebut the basis of the Examiner's assertion of inoperability, were not sufficient to show operability, or to rebut the Examiner's assertion.

Indeed, with respect to the text of each of the rejections in the present Office Action which were maintained (i.e., the rejection under 35 U.S.C. § 101 and 35 U.S.C. § 103), the above statement at paragraph 5 of the present Office Action was the only difference from the Response to Arguments of the previous Office Action mailed on September 16, 2005. Moreover, the text of the rejections under 35 U.S.C. § 101 and 35 U.S.C. § 103 was identical to the rejections set forth in the previous Office Action.

Thus, Appellants submit that the March 7, 2006 Office Action failed to advance the prosecution of the present application.

Even assuming *arguendo* that the above statement at paragraph 5 of the present Office Action satisfied the requirement for responding to the traversal positions for the rejection under 35 U.S.C. § 101, the Office Action mailed March 7, 2006 clearly failed to take note of or answer the substance of Applicant's traversal positions with respect to the rejection under 35 U.S.C. § 103.

Appellants note that, where Appellants traverse any rejections, the Examiner should, if he repeats the rejection, take note of the Appellants' argument and answer the substance of it (see M.P.E.P. § 707.07(f)).

The importance of answering Appellant's arguments is illustrated by In re Herrmann, 261 F.2d 598, 120 USPQ 182 (CCPA 1958) where the applicant urged that the subject matter claimed produced new and useful results. The court noted that since applicant's statement of advantages was not questioned by the examiner or the Board of Appeals, it was constrained to accept the statement at face value and therefore found certain claims to be allowable. See also In re Soni, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995) (Office failed to rebut applicant's argument).

In the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, Appellants clearly rebutted each of the Examiner's positions. However, the Examiner did not take note of, or answer the substance of, Appellants' traversal arguments, with the exception of the statement mentioned above.

Appellants respectfully submit that the Examiner should have responded to all of Appellants' traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

That is, the Examiner should have responded to each of Appellants' traversal positions with respect to the rejection under 35 U.S.C. § 101 on pages 16-19 of the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005.

Moreover, the Examiner should have responded to each of Appellants' traversal positions with respect to the rejection under 35 U.S.C. § 103 on pages 21-26 of the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005.

For at least the foregoing reasons, Appellants submit that the March 7, 2006 Office Action failed to advance the prosecution of the present application.

2. REJECTION UNDER 35 U.S.C. § 101

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility. That is, the Examiner asserts that the claimed invention "*could not work*", as evidenced by the Handbook of Applied Cryptography.

Appellants respectfully disagree with each of the Examiner's positions, for the following reasons.

a) OFFICE ACTION DOES NOT RESPOND TO, OR ANSWER THE SUBSTANCE OF, APPELLANTS' TRAVERSAL POSITIONS

First, as mentioned above, the Examiner's Response to Arguments is identical to the previous Response to Arguments, except for stating that "*[t]he Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands*" (see Office Action at page 2, paragraph 5), as mentioned above.

However, Appellants respectfully submit that such is not sufficient for responding to each of Appellants' traversal positions or answering the substance of those positions (e.g., see M.P.E.P. § 707.07(f) and § 2144.08(III)).

Hence, Appellants respectfully submit that the Examiner should have responded to all of Appellants' traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

b) EXAMINER IS NOT CONSIDERING APPELLANTS' ACTUAL ARGUMENT OR THE ACTUAL DISCLOSURE OF THE INVENTION

Second, Appellants respectfully submit that the Examiner is misunderstanding the invention and Appellants' traversal arguments. Moreover, the Examiner has misapplied the teachings of the Handbook of Applied Cryptography, in view of this apparent misunderstanding of Appellants' traversal position.

Appellants submit that the disclosure of the present application **explicitly acknowledges** the problem that a simple hash function approach would not work (as disclosed in the above Handbook and as suggested by the Examiner in the March 7, 2006 Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

Specifically, the specification of the present application (at page 16, lines 15-17) states that:

> Because *P0* is in general (possibly) slightly different form *Pi* for *i>0*, the secret version of *p0* will generally be quite different from the secret version of *Pi*. This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data **under uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods **to circumvent the above situation** and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe a first exemplary method, a second exemplary method, and a third exemplary method **for circumventing the very problem** with comparing encrypted or hash data, which the Examiner mentions in the Office Action.

Thus, the Examiner's continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section 9.2.2 Basis Properties and Definitions clearly is erroneous, as a matter of both fact and law. That is, the Examiner has failed to consider the specific disclosure of the present application, which clearly describes a novel **solution for circumventing the problem** being relied upon by the Examiner in the Handbook of Applied Cryptography.

Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of **circumventing** the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

Indeed, the Examiner has erroneously interpreted what the invention teaches in a way that clearly does not comport with the actual disclosure of the present application.

For example, in paragraph 11 of the March 7, 2006 Office Action, the Examiner states that the claims "*generally relate to ...*". Thus, the Examiner appears to have improperly attempted to distill the invention down to a gist of the invention.

However, the Examiner's position clearly fails to consider all of the teachings of the invention (i.e., the actual disclosure of the present application), or for that matter, the specific features recited in the claims.

As Appellants have explained in each of the previous Amendments, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

(The traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, and the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005 are incorporated herein by reference in their entirety.)

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Indeed, the claimed invention does not merely "generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication", as alleged by the Examiner.

That is, the claimed invention does NOT use a hash function by ITSELF to authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Moreover, not all of the claims deal with imperfect biometric data. Instead, only some of the claims deal with such imperfect data.

For the foregoing reasons, Appellants respectfully submit that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Appellants respectfully submit that claims 1, 14-16, 31, and 32:

> **(1)** are supported by a specific and substantial asserted utility or a well established utility,
>
> **(2)** are not inoperative and do not lack utility, and
>
> **(3)** could (and do) work for their intended purpose, as disclosed in the disclosure of the specification of the present application, for example, at page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

The Examiner has not explained why the Examiner doubts the truth or veracity of Appellants' disclosure.

To summarize, the Examiner clearly has not responded to all of Appellants' traversal positions or answered the substance of the above traversal arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)). Moreover, the Examiner appears to have erroneously summarized the teachings of the present invention in a way which clearly does not comport with the actual disclosure of the invention. Indeed, the present invention clearly is not contrary to the teachings of the Handbook of Applied Cryptography, but instead, acknowledges the very problem identified in the Handbook by the Examiner and provides a novel solution for circumventing such problems.

Thus, the Examiner's assertion that "Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands" (see Office Action at page 2, paragraph 5) clearly is inappropriate, and indeed, is not germane to the rejections since the Examiner has not explained or provided any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

For the foregoing reasons, Appellants respectfully submit that a person of ordinary skill in the art to which the invention pertains would recognize the utility of the claimed invention and would know and understand the claimed invention. Thus, the Examiner is requested to reconsider and withdraw this rejection.

3. THE PRIOR ART REJECTION

Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon. Appellants respectfully traverse this rejection, for at least the following reasons.

As mentioned above, the traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, and the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005 are incorporated herein by reference in their entirety.

a) THE CLAIMED INVENTION

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P').

Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

b) EXAMINER'S RESPONSE TO ARGUMENTS

In the "Response to Arguments" section of the Office Action, the Examiner continues to allege that the features upon which Appellants rely are not recited in the claims (see Office Action at page 3, paragraph 6). However, Appellants submit that the traversal arguments which are set forth at least in the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005 and the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, clearly point out the claimed subject matter which is clearly and particularly defined, for example, by independent claim 1.

Also, in the "Response to Arguments" section of the Office Action, the Examiner relies on M.P.E.P. § 2122 as stating that, when a reference relied upon expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable.

c) EXAMINER'S POSITION IS FLAWED AS A MATTER OF FACT AND LAW

Appellants respectfully submit that the Examiner's position is flawed as a matter of fact and law.

First, as Appellants have pointed out, Borza does not expressly anticipate or make obvious all of the elements of the claimed invention. Thus, irrespective of the operability of Borza, Appellants submit that the alleged combination of Borza and Kharon does not disclose or suggest all of the features of the claimed invention.

Instead, Borza only generally mentions that a comparison of encrypted data is done, but does not disclose the specific features recited in the claimed invention. In fact, Borza clearly does not discuss *how* it compares encrypted data.

In fact, the cited portion of Borza at column 16, lines 31-38 does not determine whether h(P) is close to h(P'), as alleged by the Examiner. Indeed, it is unclear how Borza at column 16, lines 31-38 even relates to the disclosure of comparing encrypted data against an encrypted template at column 8, lines 28-38.

That is, nowhere at column 16, lines 31-38, or in Figure 13 which is being described therein, does Borza mention comparing encrypted data against an encrypted template. Thus, the Examiner has mischaracterized the teachings of Borza.

Second, even assuming *arguendo* that Borza is operative, the disclosure provided by Borza fails to teach or suggest all of the features of the claimed invention for which it is being relied upon. Therefore, the alleged combination of Borza and Kharon clearly does not disclose or suggest all of the features of the claimed invention.

In other words, irrespective of the operability of Borza, the disclosure of Borza clearly does not disclose or suggest *how* to compare two encrypted data sets to determine similarity between the two original data sets according to the features recited in the claimed invention.

Appellants reiterate that the ordinarily skilled artisan would understand that encryption causes diffusion of data, which means that the encryption of two similar, but not identical data sets create two encrypted data sets that are very different. Thus, merely comparing two encrypted data sets still would not (and does not) disclose or suggest the similarity between the two unencrypted data sets.

In fact, as the Examiner points out, and as Appellants specifically acknowledge in the specification, no identification is possible by direct comparison of the encrypted data.

Thus, in contrast to Borza, the claimed invention discloses several approaches to compare encrypted or hashed data **under such uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

Specifically, as mentioned above, the disclosure of the present invention specifically acknowledges the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

For example, the specification of the present application (at page 16, lines 15-17) specifically states that:

> Because *P0* is in general (possibly) slightly different form *Pi* for *i>0*, the secret version of *p0* will generally be quite different from the secret version of *Pi*. This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data **under such uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods **to circumvent this situation** and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first, second, and third methods for circumventing the very problem with comparing encrypted or hash data which the Examiner mentions.

The claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

The present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template *under the possibility that the data might be slightly different from the template* (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the claimed invention solves the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17) by circumventing the problem, as disclosed and claimed.

For the foregoing reasons, Borza clearly does not disclose or suggest at least "*to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P*", as recited in claim 1.

Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 recite somewhat similar features. Therefore, Appellants submit that Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 also are patentable over the prior art of record for the same reasons as independent claim 1.

On the other hand, Appellants respectfully reiterate that Kharon does not make up for the deficiencies of Borza.

The Examiner relies on Kharon for teaching the claimed "*extracting sub-collections Sj from the collection of data in data set P; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred*", as recited in independent claim 1.

However, contrary to the Examiner's position, Kharon (at column 13, lines 43-67) does not describe extracting multiple subsets Sj (i.e., "*sub-collections*") from the data. Furthermore, Kharon does not describe encrypting a number of such subsets (i.e., a "*number of such sub-collections*") such that at least one is reproduced exactly with a predetermined probability.

Appellants respectfully submit that the Examiner seems to have confused using a smaller section of the data for verification (which would be less desirable since less data is used), whereas the claimed invention uses multiple subsets of the data for verification.

Thus, using just a smaller subset of the data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data.

On the other hand, using multiple subsets of the data, according to the claimed invention, allows encrypted data to be compared and to generate a measure of similarity.

Thus, for the foregoing reasons, Appellants respectfully submit that Borza and Kharon, either individually or in combination, discloses or suggests all of the features of the claimed invention. Therefore, the Examiner is requested to reconsider and withdraw this rejection.

In view of all of the foregoing, Appellants submit that all of the pending claims (i.e., claims 1 and 5-36) are patentable over the prior art of record.

VIII. CONCLUSION

In view of the foregoing, Appellants submit that Claims 1 and 5-36 of the application are patentably distinct from the prior art of record and in condition for allowance. Thus, the Board is respectfully requested to remove the rejections of Claims 1 and 5-36.

Please charge any deficiencies and/or credit any overpayments necessary to enter this paper to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: February 20, 2007

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY
LAW GROUP, PLLC**
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via USPTO Electronic Filing System (EFS) the enclosed Corrected Appellants' Brief on Appeal, on February 20, 2007.

John J. Dresch, Esq.
Registration No. 46,672

CLAIMS APPENDIX

1. A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P;

storing h(P) in a database, and

obtaining a sample of P’ such that a comparison can be made;

at least one of obtaining and computing h(P’); and

to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,

wherein said data set P cannot be extracted from h(P),

wherein said semiotic data comprises biometric data,

wherein said function h comprises a secure hash function,

wherein the data set P is not determined perfectly by its reading, wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred,

each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database, wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and

wherein at least one of said data set P and P' comprises a personal data set.

5. A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P; and

storing h(P) in a database,

wherein said data set P cannot be extracted from h(P),

the method further comprising:

selecting a private key/public key (K, k) once for all cases; and

one of destroying said private key K and sending said private key K to a trusted party; and

choosing said function h as the public encryption function corresponding to k.

6. The method according to claim 5, wherein said data set P cannot be extracted from h(P), except by the trusted party.

7. The method according to claim 5, further comprising:

to determine whether some P' is a predetermined subject, comparing said h(P') to available h(P)s; and

determining whether there is a match.

8. The method according to claim 5, wherein the trusted party comprises a panel of members, and

wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret.

9. A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P; and

storing h(P) in a database,

wherein said data set P cannot be extracted from h(P), wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data.

10. The method according to claim 9, further comprising:

extracting sub-collections Sj from the collection of data in data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

11. The method according to claim 10, further comprising:

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

12. The method according to claim 11, further comprising:

each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

13. The method according to claim 12, wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user.

14. The method according to claim 1, wherein at least one of said data set P and P' comprises a personal data set.

15. A method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired;

destroying the unencrypted data set P;

storing each of the at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether the data set P' substantially matches, but does not exactly match, the at least one encrypted data set stored in the database.

16. The method according to claim 15, wherein at least one of said data set P and P' comprises a personal data set.

17. A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match.

18. The method according to claim 17, wherein at least one of said data set P and P' comprises a personal data set.

19. A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

20. The method according to claim 19, wherein said data set comprises a personal data set.

21. The method according to claim 19, further comprising:

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

22. The method according to claim 21, wherein a data set P is not determined perfectly by its reading, such that each reading gives a number Pi,

wherein i is no less than 0,

wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data.

23. The method according to claim 21, further comprising:

each time a data set is read Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

24. A system for processing semiotic data, comprising:

means for receiving semiotic data including a data set P;

means for selecting a function h, and for each said data set P to be collected, computing h(P);

means for destroying said data set P;

means for storing h(P) in a database, wherein said data set P cannot be extracted from h(P), and

to determine whether a data set P' is close to a predetermined subject, means for comparing h(P') to available h(P)s to determine whether data set P' is close to some P.

25. A system of processing semiotic data as in claim 24, wherein said semiotic data comprises biometric data.

26. The system according to claim 24, wherein at least one of said data set P and P' comprises a personal data set.

27. A system for verifying biometric data without storing unencrypted biometric data, comprising:

means for acquiring unencrypted biometric data including at least one data set P;

means for encrypting each said at least one data set acquired to form at least one encrypted data set; means for destroying the unencrypted data set P;

means for storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

means for comparing an encrypted data set of a data set P' to said at least one encrypted data set of data set P to determine whether there is a match and to determine whether the data set P' is a predetermined subject.

28. The system according to claim 27, wherein at least one of said data set P and P' comprises a personal data set.

29. A system for extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

30. The system according to claim 29, wherein said data set comprises a personal data set.

31. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented processing biometric data, said method comprising:

receiving biometric data including a data set P;

selecting a secure hash function h, and for each data set P to be collected, computing h(P);

destroying said data set P;

storing h(P) in a database, wherein said data set P cannot be extracted from h(P), and

to determine whether a data set P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether data set P' is close to some data set P.

32. The signal-bearing medium according to claim 31, wherein at least one of said data set P and P' comprises a personal data set.

33. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented verifying of biometric data without storing unencrypted biometric data, said method comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is close to a predetermined subject, comparing an encrypted data set of P' to said at least one encrypted data set to determine whether data set P' is close to some data set P.

34. The signal-bearing medium according to claim 33, wherein at least one of said data set P and P' comprises a personal data set.

35. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented extracting components of biometric data which are stable under measurement errors, said method comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database;

extracting sub-collections Sj from the collection of data in said data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

36. The signal-bearing medium according to claim 35, wherein said data set comprises a personal data set.

EVIDENCE APPENDIX

Not applicable.

RELATED PROCEEDINGS APPENDIX

Not applicable.